Mathematical Surveys and Monographs

Volume 278

Applications of Group Theory in Cryptography

Post-quantum Group-based Cryptography

Delaram Kahrobaei
Ramón Flores
Marialaura Noce
Maggie E. Habeeb
Christopher Battarbee

10.1090/surv/278

Applications of Group Theory in Cryptography

Post-quantum Group-based Cryptography

Mathematical
Surveys
and
Monographs

Volume 278

Applications of Group Theory in Cryptography

Post-quantum Group-based Cryptography

Delaram Kahrobaei
Ramón Flores
Marialaura Noce
Maggie E. Habeeb
Christopher Battarbee

AMS American Mathematical Society
Providence, Rhode Island

EDITORIAL COMMITTEE

Alexander H. Barnett
Michael A. Hill
Bryna Kra (chair)
David Savitt
Natasa Sesum
Jared Wunsch

2020 *Mathematics Subject Classification*. Primary 94A60, 81P94, 20F05, 20F99, 20F10.

For additional information and updates on this book, visit
www.ams.org/bookpages/surv-278

Library of Congress Cataloging-in-Publication Data

Names: Kahrobaei, Delaram, 1975- author. | Flores, Ramón, 1975- author. | Noce, Marialaura, 1992- author. | Habeeb, Maggie E., 1983- author. | Battarbee, Christopher, 1998- author.
Title: Applications of group theory in cryptography : post-quantum group-based cryptography / Delaram Kahrobaei, Ramón Flores, Marialaura Noce, Maggie E. Habeeb, Christopher Battarbee.
Description: Providence, Rhode Island : American Mathematical Society, [2024] | Series: Mathematical surveys and monographs, 0076-5376 ; volume 278 | Includes bibliographical references and index.
Identifiers: LCCN 2023044735 | ISBN 9781470474690 (paperback) | ISBN 9781470476212 (ebook)
Subjects: LCSH: Group theory. | Cryptography. | AMS: Information and communication, circuits – Communication, information – Cryptography. | Quantum theory – Axiomatics, foundations, philosophy – Quantum cryptography. | Group theory and generalizations – Special aspects of infinite or finite groups – Generators, relations, and presentations. | Group theory and generalizations – Special aspects of infinite or finite groups – None of the above, but in this section. | Group theory and generalizations – Special aspects of infinite or finite groups – Word problems, other decision problems, connections with logic and automata.
Classification: LCC QA174.2 .K34 2024 | DDC 652/.8015122–dc23/eng20231103
LC record available at https://lccn.loc.gov/2023044735

Color graphic policy. Any graphics created in color will be rendered in grayscale for the printed version unless color printing is authorized by the Publisher. In general, color graphics will appear in color in the online version.

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy select pages for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for permission to reuse portions of AMS publication content are handled by the Copyright Clearance Center. For more information, please visit `www.ams.org/publications/pubpermissions`.

Send requests for translation rights and licensed reprints to `reprint-permission@ams.org`.

© 2024 by the American Mathematical Society. All rights reserved.
The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

⊗ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `https://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 29 28 27 26 25 24

To the memories of Gilbert Baumslag and Benjamin Fine
and to Michael Anshel

Contents

Introduction xi

Acknowledgments xv

Notation xvii

Part 1. Background Information 1

Chapter 1. Group Theory 3
1.1. Introduction 3
1.2. Basic definitions and examples 3
1.3. Examples of groups 4
1.4. Subgroups and order of elements 5
1.5. Normal subgroups and quotients 6
1.6. Group actions 8
1.7. Extensions 8
1.8. Nilpotent groups 10

Chapter 2. Algorithmic Problems in Group Theory 13
2.1. Introduction 13
2.2. Combinatorial group theory 13
2.3. Decision problems in groups 15
2.4. Search problems 16
2.5. Algorithmic problems in graphs and groups 16
2.6. Other problems in groups 18

Chapter 3. Classical Cryptography 21
3.1. Introduction 21
3.2. Digital signature schemes 25
3.3. Secret sharing schemes 27
3.4. Multilinear maps 28

Part 2. Post-quantum Cryptography and Cryptanalysis 31

Chapter 4. Noncommutative Cryptographic Protocols 33
4.1. Noncommutative key exchange protocols 33
4.2. Noncommutative digital signatures 38
4.3. Noncommutative secret sharing schemes 41

Chapter 5. Attacks 47
5.1. Introduction 47
5.2. Length-based attack 47
5.3. Linear centralizer attack 49
5.4. Linear decomposition attack 50
5.5. Quotient attack 51

Chapter 6. Quantum Cryptanalysis 53
6.1. Introduction 53
6.2. The hidden subgroup problem 54
6.3. Relation of HSP to other computational problems 57
6.4. Quantum cryptanalysis for group-based PQC 58

Part 3. Cryptographic Platforms 63

Chapter 7. Braid Groups 65
7.1. Introduction 65
7.2. Mathematical background 65
7.3. Algorithmic problems 69
7.4. Cryptographic protocols 72

Chapter 8. Hyperbolic Groups 75
8.1. Introduction 75
8.2. Mathematical background 75
8.3. Algorithmic problems 79
8.4. Cryptographic protocols 82

Chapter 9. Small Cancellation Groups 85
9.1. Introduction 85
9.2. Mathematical background 85
9.3. Algorithmic problems 87
9.4. Cryptographic protocols 89

Chapter 10. Polycyclic Groups 93
10.1. Introduction 93
10.2. Mathematical background 93
10.3. Algorithmic problems 96
10.4. Cryptographic protocols 97

Chapter 11. Graph Groups 101
11.1. Introduction 101
11.2. Mathematical background 101
11.3. Algorithmic problems 103
11.4. Cryptographic protocols 105
11.5. Interesting problems 106

Chapter 12. Arithmetic Groups 109
12.1. Introduction 109
12.2. Mathematical background 109
12.3. Algorithmic problems 111
12.4. The protocol 112

Chapter 13. Engel Groups 115
13.1. Introduction 115
13.2. Mathematical background 115
13.3. Cryptographic protocols 118
13.4. Interesting problems 119

Chapter 14. Self-Similar Groups 121
14.1. Introduction 121
14.2. Mathematical background 121
14.3. Algorithmic problems 125
14.4. Cryptographic protocols 126

Bibliography 129

Index 139

Introduction

Group-based cryptography is a very recent and fast-growing field of research at the intersection of group theory, combinatorics, complexity theory, coding theory, and cryptology. The main goal of group-based cryptography is the development and analysis of secure cryptographic protocols using as input algorithmic properties of different classes of groups, and in particular the complexity of decision and search problems in finitely generated groups. In general these techniques are especially useful in public-key cryptography, which provides a method for two parties to communicate privately, despite the lack of any prearranged security keys.

The methodology of group-based cryptography follows the usual pattern of showing that a *break* to a cryptosystem amounts to the solution of a difficult mathematical problem. Indeed, one can think of the very first examples of public-key cryptography as *group-based* — after all, the famous problems of integer factorization or recovering discrete logarithms can be thought of as group-theoretic problems, and cryptosystems based on these problems retain a vital role in modern digital infrastructure. However, with the advent of quantum computers, these underlying mathematical problems are efficiently solvable, and hence the corresponding cryptographic schemes are deemed insecure in this setting. In the post-quantum era different tools are required: in this direction, in 2015, the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) announced an initiative for the development of post-quantum cryptosystems. Lattice-based, code-based, multivariate-based, and hash-based primitives where shortlisted as third-round finalists suggested for standardization five years later [**170**]; nevertheless, since the announcement some of these finalists have been the subject of major cryptanalytic work — in some cases casting the viability of these schemes as post-quantum standards into serious doubt. In light of these developments it remains vital to study a diverse range of computational problems; a promising class of such tools comes from group-based cryptography. In fact, not only does this theory offer a rich supply of complex and varied problems for cryptography; reciprocally, the study of cryptographic algorithms built from these problems has contributed results to computational group theory.

In the following we provide a nonexhaustive but very significant list of families of groups which have been considered as platforms for different security protocols: braid groups ([**2**] and [**131**]), polycyclic groups [**46**], matrix groups [**90**], nonabelian simple groups [**174**], hyperbolic groups [**30**], arithmetic groups [**118**], graph groups [**61**], nilpotent groups [**122**], automata groups ([**71**], [**86**]), Thompson groups [**127**], free metabelian groups [**197**], small cancellation groups [**97**], free nilpotent p-groups [**120**], Engel groups [**119**], or infinite pro-p groups [**121**]. Many of these families are discussed in the last part of the book.

Computational problems thought to be difficult in these groups give rise, in turn, to a number of cryptographic protocols. Among them, we quote here the group-based digital signature WalnutDSA^{TM} [**3**], which has faced several attacks ([**99**], [**13**], [**136**]) and is claimed by the authors to be quantum-resistant; the AAG key exchange protocol [**2**]; a noncommutative version of Diffie-Hellman [**131**]; homomorphic encryption schemes ([**90**], [**174**]), hash functions [**177**], multilinear maps [**122**], noncommutative secret-sharing schemes ([**175**], [**97**]), authentication schemes [**60**], or asymmetric key exchange protocols [**30**]. These schemes, and their corresponding cryptanalysis, are the subject of Part II of the book. We also provide a brief overview of quantum cryptanalysis for group-based cryptography, including Shor's algorithm [**194**] and Kuperberg's algorithm for the dihedral hidden subgroup problem [**139**]. Moreover, some of the techniques are used to establish a strong connection to the area of group-based cryptography established in [**36**].

Our book is intended to be a comprehensive introduction to group-based cryptography. We note that there already exist thorough references on the subject, such as the monographs of Myasnikov-Shpilrain-Ushakov [**160**] and [**162**]. Our treatment is not so exhaustive, as we aim to offer a friendly approach which is accessible to both computer scientists and mathematicians. With this goal in mind, we have tried to present the group-theoretic statements and proofs in the easiest way, avoiding unnecessary technicalities and preferring, in general, the combinatorial versions of the results; in turn, we have been very descriptive when developing the protocols, the algorithms, and the cryptanalysis. On the other hand, our intention has also been to present the most updated version of the subject, with special attention to the protocols and references of the last years. If we have achieved the goal of adding a new item to the bibliography where the material is accessible and completely updated, we will be satisfied as authors.

We conclude this introduction by providing a detailed description of the contents of our book.

Organization of the book. The book is divided into three parts. The first one provides background information and basic notions of group theory, algorithmic problems in groups, and classical cryptography. More precisely, in Chapter 1, we survey the basic theory of groups, subgroups, and special classes of groups such as cyclic and nilpotent groups. In this part, we also describe free groups and combinatorial group theory. Chapter 2 lays the groundwork for describing algorithmic problems in group theory: we describe group-theoretic decision problems including the word, conjugacy, and isomorphism decision problems. We also describe the power decision problem, the endomorphism decision problem, the n-th root decision problem, and the geodesic length decision problem. We also present many search problems. In Chapter 3 we describe a number of cryptosystems that have been built around several classes of groups in the last decades. In particular, we present digital signature schemes, secret sharing schemes, and multilinear maps.

Part 2 is devoted to group-theoretic post-quantum cryptography. In Chapter 4 we present several key exchange protocols based on an underlying noncommutative structure such as Anshel-Anshel-Goldfeld (AAG) key exchange, Ko, Lee, et al. key exchange, and the noncommutative ElGamal key exchange. We also introduce two key exchange protocols based on the semidirect product of groups or semigroups. A discussion of noncommutative digital signatures, such as the Kahrobaei-Koupparis digital signature scheme and the Mohan and Anjaneyulu digital signature scheme,

and of noncommutative secret sharing schemes is also included. We discuss the Panagopoulos threshold scheme as it has motivated the construction of some noncommutative threshold schemes. These include the Habeeb-Kahrobaei-Shpilrain (HKS) secret sharing scheme, which is a hybrid of Shamir's secret sharing scheme that provides some advantages to Shamir's scheme, and threshold schemes based on Nielsen transformations. Chapter 5 introduces some recent attacks against these schemes: for example the length-based attack, the linear centralizer attack, the linear decomposition attack, and the quotient attack. Chapter 6 deals with quantum cryptanalysis of some examples of group-based cryptography, in particular as it relates to complexity of the hidden subgroup problem (HSP). We cover the famous construct of Shor's algorithm and survey the state of the art for quantum algorithms addressing the hidden subgroup problem in groups not accounted for by Shor's algorithm. Finally, we provide a "case study"-type exposition of two recent results in group-based quantum cryptanalysis.

The last part of the book is devoted to suitable platforms for the cryptographic protocols presented in Part 2. In each chapter we give the definition of the class of groups proposed together with important properties and the status of their algorithmic problems. Then, we survey the current status of the respective group in cryptography, and we also include a list of open problems, which we hope will guide researchers who wish to work in this field. The groups that we propose as cryptographic platforms are the following: braid groups, hyperbolic groups, small cancellation groups, polycyclic groups, graph groups, arithmetic groups, Engel groups, and self-similar groups.

Acknowledgments

Delaram Kahrobaei: Over the years, this research has been supported, in various forms, by grants from the National Science Foundation (NSF), the Office of Naval Research, Canada's New Frontiers in Research Fund (NFRF)-Exploration stream, the American Association for the Advancement of Science (AAAS), and the London Mathematical Society (LMS). The first author is grateful to the Institut des Hautes Études Scientifiques (IHES) for providing excellent scientific environment to do mathematics, this article was finished during her visit to IHES.

Ramón Flores: We warmly thank Y. Antolín and J. González-Meneses for helpful comments. The second author was partially supported by grant PID2020-117971GB-C21 from the Spanish Ministry for Science and Innovation (MCIN), and grant FQM-213 from the Junta de Andalucía.

Notation

Throughout the book we will use standard notation and terminology (see [**186**]). We often consider nonabelian groups with multiplicative notation, in which the multiplication symbol is always omitted. In the following table G always denotes a group.

Groups	
Trivial element of G	e, 1, 1_G
G is isomorphic to K	$G \simeq K$
H is a subgroup of G	$H \leq G$
Subgroup generated by X in G	$\langle X \rangle$
Normal closure of X in G	$\langle X \rangle^G$
The index of a subgroup H in G	$\lvert G : H \rvert$
g and h are conjugate elements	$g^h = h^{-1}gh$
Commutator of elements h and g	$[h, g] = h^{-1}g^{-1}hg$
Commutator of two sets A and B	$[A, B]$
Commutator (or derived) subgroup of G	$G' = [G, G]$
Center of G	$Z(G)$
Centralizer of a set X in G	$C_G(X)$
Normalizer of a set X in G	$N_G(X)$

Bibliography

[1] G. Alagic and A. Russell, *Quantum-secure symmetric-key cryptography based on hidden shifts*, Advances in cryptology—EUROCRYPT 2017. Part III, Lecture Notes in Comput. Sci., vol. 10212, Springer, Cham, 2017, pp. 65–93, DOI 10.1007/978-3-319-56617-7_3. MR3652147

[2] I. Anshel, M. Anshel, and D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Lett. **6** (1999), no. 3-4, 287–291, DOI 10.4310/MRL.1999.v6.n3.a3. MR1713130

[3] I. Anshel, D. Atkins, D. Goldfeld, and P. E. Gunnells, *WalnutDSA$^{\mathrm{TM}}$: a group theoretic digital signature algorithm*, Int. J. Comput. Math. Comput. Syst. Theory **6** (2021), no. 4, 260–284, DOI 10.1080/23799927.2020.1831613. MR4355498

[4] Y. Antolín and A. W. Sale, *Permute and conjugate: the conjugacy problem in relatively hyperbolic groups*, Bull. Lond. Math. Soc. **48** (2016), no. 4, 657–675, DOI 10.1112/blms/bdw028. MR3532141

[5] L. Babai, *Group, graphs, algorithms: the graph isomorphism problem*, Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. IV. Invited lectures, World Sci. Publ., Hackensack, NJ, 2018, pp. 3319–3336. MR3966534

[6] R. Baer, *Engelsche elemente Noetherscher Gruppen*, Math. Ann. **133** (1957), 256–270, `https://doi.org/10.1007/BF02547953`.

[7] J. Barnard, N. Brady, and P. Dani, *Super-exponential distortion of subgroups of CAT(−1) groups*, Algebr. Geom. Topol. **7** (2007), 301–308, DOI 10.2140/agt.2007.7.301. MR2308946

[8] L. Bartholdi, *Endomorphic presentations of branch groups*, J. Algebra **268** (2003), no. 2, 419–443, DOI 10.1016/S0021-8693(03)00268-0. MR2009317

[9] L. Bartholdi, R. I. Grigorchuk, and Z. Šuniḱ, *Branch groups*, Handbook of algebra, Vol. 3, Handb. Algebr., vol. 3, Elsevier/North-Holland, Amsterdam, 2003, pp. 989–1112, DOI 10.1016/S1570-7954(03)80078-5. MR2035113

[10] C. Battarbee, D. Kahrobaei, and S. F. Shahandashti, *Cryptanalysis of semidirect product key exchange using matrices over non-commutative rings*, Mathematical Cryptology **1** (2021), no. 1, 1–8.

[11] C. Battarbee, D. Kahrobaei, L. Perret, and S. F Shahandashti, *A subexponential quantum algorithm for the semdirect discrete logarithm problem*, arXiv preprint arXiv:2209.02814 (2022).

[12] G. Baumslag, N. Fazio, A. R. Nicolosi, V. Shpilrain, and W. E. Skeith III, *Generalized learning problems and applications to non-commutative cryptography (extended abstract)*, Provable security, Lecture Notes in Comput. Sci., vol. 6980, Springer, Heidelberg, 2011, pp. 324–339, DOI 10.1007/978-3-642-24316-5_23. MR2911480

[13] W. Beullens and S. R. Blackburn, *Practical attacks against the walnut digital signature scheme*, Advances in cryptology—ASIACRYPT 2018. Part I, Lecture Notes in Comput. Sci., vol. 11272, Springer, Cham, 2018, pp. 35–61, DOI 10.1007/978-3-030-03326-2_2. MR3897822

[14] J. S. Birman, *Braids, links, and mapping class groups*, Annals of Mathematics Studies, No. 82, Princeton University Press, Princeton, NJ; University of Tokyo Press, Tokyo, 1974. MR375281

[15] J. S. Birman, K. H. Ko, and S. J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. **139** (1998), no. 2, 322–353, `https://doi.org/10.1006/aima.1998.1761`. MR1654165

[16] D. Boneh and R. J. Lipton, *Quantum cryptanalysis of hidden linear functions (extended abstract)*, Advances in cryptology—CRYPTO '95 (Santa Barbara, CA, 1995), Lecture Notes in Comput. Sci., vol. 963, Springer, Berlin, 1995, pp. 424–437, DOI 10.1007/3-540-44750-4_34. MR1445578

[17] D. Boneh and A. Silverberg, *Applications of multilinear forms to cryptography*, Topics in algebraic and noncommutative geometry (Luminy/Annapolis, MD, 2001), 2003, pp. 71–90, https://doi.org/10.1090/conm/324/05731.

[18] A. Borel, *Introduction aux groupes arithmétiques* (French), Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341, Hermann, Paris, 1969. MR244260

[19] M. R. Bridson, *On the subgroups of right-angled Artin groups and mapping class groups*, Math. Res. Lett. **20** (2013), no. 2, 203–212, DOI 10.4310/MRL.2013.v20.n2.a1. MR3151642

[20] M. R. Bridson and A. Haefliger, *Metric spaces of non-positive curvature*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 319, Springer-Verlag, Berlin, 1999, DOI 10.1007/978-3-662-12494-9. MR1744486

[21] M. R. Bridson and J. Howie, *Conjugacy of finite subsets in hyperbolic groups*, Internat. J. Algebra Comput. **15** (2005), no. 4, 725–756, DOI 10.1142/S0218196705002529. MR2160576

[22] D. R. L. Brown, N. Koblitz, and J. T. LeGrow, *Cryptanalysis of "MAKE"*, J. Math. Cryptol. **16** (2022), no. 1, 98–102, DOI 10.1515/jmc-2021-0016. MR4378544

[23] S. Burckel, *The well-ordering on positive braids*, J. Pure Appl. Algebra **120** (1997), no. 1, 1–17, DOI 10.1016/S0022-4049(96)00072-2. MR1466094

[24] W. Burnside, *On an unsettled question in the theory of discontinous groups*, Quart. J. Pure Appl. Math. **33** (1902), 230–238.

[25] M. Casals-Ruiz, *Embeddability and quasi-isometric classification of partially commutative groups*, Algebr. Geom. Topol. **16** (2016), no. 1, 597–620, DOI 10.2140/agt.2016.16.597. MR3470711

[26] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, *CSIDH: an efficient post-quantum commutative group action*, Advances in cryptology—ASIACRYPT 2018. Part III, Lecture Notes in Comput. Sci., vol. 11274, Springer, Cham, 2018, pp. 395–427, DOI 10.1007/978-3-030-03332-3_15. MR3897883

[27] B. Cavallo and D. Kahrobaei, *Secret sharing using non-commutative groups and the shortlex order*, Algorithmic problems of group theory, their complexity, and applications to cryptography, Contemp. Math., vol. 633, Amer. Math. Soc., Providence, RI, 2015, pp. 1–8, DOI 10.1090/conm/633/12646. MR3364217

[28] B. Chandler and W. Magnus, *The history of combinatorial group theory: A case study in the history of ideas*, Studies in the History of Mathematics and Physical Sciences, vol. 9, Springer-Verlag, New York, 1982, DOI 10.1007/978-1-4613-9487-7. MR680777

[29] R. Charney, *An introduction to right-angled Artin groups*, Geom. Dedicata **125** (2007), 141–158, DOI 10.1007/s10711-007-9148-6. MR2322545

[30] I. Chatterji, D. Kahrobaei, and N. Y. Lu, *Cryptosystems using subgroup distortion*, Theoretical and Applied Informatics **29** (2017), no. 1-2, 14–24.

[31] J. H. Cheon and B. Jun, *A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem*, Advances in cryptology—CRYPTO 2003, Lecture Notes in Comput. Sci., vol. 2729, Springer, Berlin, 2003, pp. 212–225, DOI 10.1007/978-3-540-45146-4_13. MR2093195

[32] A. Childs, *Lecture notes on quantum algorithms, https://www.cs.umd.edu/ amchilds/qa/qa.pdf* (2017), http://www.cs.umd.edu/~amchilds/qa/qa.pdf.

[33] A. M. Childs and W. van Dam, *Quantum algorithms for algebraic problems*, Rev. Modern Phys. **82** (2010), no. 1, 1–52, https://doi.org/10.1103/RevModPhys.82.1. MR2629607

[34] A. M. Childs and G. Ivanyos, *Quantum computation of discrete logarithms in semigroups*, J. Math. Cryptol. **8** (2014), no. 4, 405–416, DOI 10.1515/jmc-2013-0038. MR3281663

[35] A. M. Childs and W. van Dam, *Quantum algorithms for algebraic problems*, Rev. Modern Phys. **82** (2010), no. 1, 1–52, DOI 10.1103/RevModPhys.82.1. MR2629607

[36] J.-M. Couveignes, *Hard homogeneous spaces*, Cryptology ePrint Archive (2006).

[37] J. Crisp, E. Godelle, and B. Wiest, *The conjugacy problem in subgroups of right-angled Artin groups*, J. Topol. **2** (2009), no. 3, 442–460, DOI 10.1112/jtopol/jtp018. MR2546582

[38] P. de la Harpe, *Topics in geometric group theory*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000. MR1786869

[39] P. Dehornoy, *A fast method for comparing braids*, Adv. Math. **125** (1997), no. 2, 200–235, DOI 10.1006/aima.1997.1605. MR1434111

[40] P. Dehornoy, *Braid-based cryptography*, Group theory, statistics, and cryptography, Contemp. Math., vol. 360, Amer. Math. Soc., Providence, RI, 2004, pp. 5–33, DOI 10.1090/conm/360/06566. MR2105432

[41] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest, *Ordering braids*, Mathematical Surveys and Monographs, vol. 148, American Mathematical Society, Providence, RI, 2008, DOI 10.1090/surv/148. MR2463428

[42] E. Di Domenico, G. A. Fernández-Alcober, M. Noce, and A. Thillaisundaram, *p-Basilica groups*, Mediterr. J. Math. **19** (2022), no. 6, Paper No. 275, 28, DOI 10.1007/s00009-022-02187-z. MR4505206

[43] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **IT-22** (1976), no. 6, 644–654, https://doi.org/10.1109/tit.1976.1055638.

[44] B. Domanski and M. Anshel, *The complexity of Dehn's algorithm for word problems in groups*, J. Algorithms **6** (1985), no. 4, 543–549, DOI 10.1016/0196-6774(85)90031-8. MR813591

[45] C. Droms, *Isomorphisms of graph groups*, Proc. Amer. Math. Soc. **100** (1987), no. 3, 407–408, https://doi.org/10.2307/2046419.

[46] B. Eick and D. Kahrobaei, *Polycyclic groups: A new platform for cryptology?*, arXiv math:0411077 (2004).

[47] B. Eick and G. Ostheimer, *On the orbit-stabilizer problem for integral matrix actions of polycyclic groups*, Math. Comp. **72** (2003), no. 243, 1511–1529, DOI 10.1090/S0025-5718-03-01493-5. MR1972750

[48] K. Eisenträger, S. Hallgren, A. Kitaev, and F. Song, *A quantum algorithm for computing the unit group of an arbitrary degree number field*, STOC'14—Proceedings of the 2014 ACM Symposium on Theory of Computing, ACM, New York, 2014, pp. 293–302. MR3238955

[49] E. A. El-Rifai and H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford Ser. (2) **45** (1994), no. 180, 479–497, https://doi.org/10.1093/qmath/45.4.479.

[50] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inform. Theory **31** (1985), no. 4, 469–472, DOI 10.1109/TIT.1985.1057074. MR798552

[51] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, *Word processing in groups*, Jones and Bartlett Publishers, Boston, MA, 1992. MR1161694

[52] D. B. A. Epstein and D. F. Holt, *The linearity of the conjugacy problem in word-hyperbolic groups*, Internat. J. Algebra Comput. **16** (2006), no. 2, 287–305, https://doi.org/10.1142/S0218196706002986. MR2228514

[53] M. Ershov, *Golod-Shafarevich groups: a survey*, Internat. J. Algebra Comput. **22** (2012), no. 5, 1230001, 68, DOI 10.1142/S0218196712300010. MR2949205

[54] B. Farb, *The extrinsic geometry of subgroups and the generalized word problem*, Proc. London Math. Soc. (3) **68** (1994), no. 3, 577–593, https://doi.org/10.1112/plms/s3-68.3.577. MR1262309

[55] D. Farley and L. Sabalka, *Discrete Morse theory and graph braid groups*, Algebr. Geom. Topol. **5** (2005), 1075–1109, https://doi.org/10.2140/agt.2005.5.1075. MR2171804

[56] N. Fazio, K. Iga, A. R. Nicolosi, L. Perret, and W. E. Skeith III, *Hardness of learning problems over Burnside groups of exponent 3*, Des. Codes Cryptogr. **75** (2015), no. 1, 59–70, https://doi.org/10.1007/s10623-013-9892-6. MR3320351

[57] G. A. Fernández-Alcober and A. Zugadi-Reizabal, *GGS-groups: order of congruence quotients and Hausdorff dimension*, Trans. Amer. Math. Soc. **366** (2014), no. 4, 1993–2017, DOI 10.1090/S0002-9947-2013-05908-9. MR3152720

[58] B. Fine, M. Habeeb, D. Kahrobaei, and G. Rosenberger, *Aspects of nonabelian group-based cryptography: a survey and open problems*, JP J. Algebra Number Theory Appl. **21** (2011), no. 1, 1–40. MR2840945

[59] B. Fine, A. Moldenhauer, and G. Rosenberger, *Cryptographic protocols based on Nielsen transformations*, Journal of Computer and Communication **4** (2016), 63–107.

[60] R. Flores and D. Kahrobaei, *Cryptography with right-angled Artin groups*, Theoretical and Applied Informatics **28** (2016), no. 3, 8–16.

[61] R. Flores, D. Kahrobaei, and T. Koberda, *Algorithmic problems in right-angled Artin groups: complexity and applications*, J. Algebra **519** (2019), 111–129, DOI 10.1016/j.jalgebra.2018.10.023. MR3874519

[62] R. Flores, D. Kahrobaei, and T. Koberda, *A cryptographic application of the Thurston norm*, Int. J. Comput. Math. Comput. Syst. Theory **5** (2020), no. 1, 15–24, DOI 10.1080/23799927.2020.1716074. MR4095613

[63] R. Flores, D. Kahrobaei, and T. Koberda, *Expander graphs and right-angled Artin groups*, arXiv 2005:06143 (2022).

[64] E. Formanek, *Conjugate separability in polycyclic groups*, J. Algebra **42** (1976), no. 1, 1–10, DOI 10.1016/0021-8693(76)90021-1. MR419608

[65] N. Franco and J. González-Meneses, *Conjugacy problem for braid groups and Garside groups*, J. Algebra **266** (2003), no. 1, 112–132, DOI 10.1016/S0021-8693(03)00292-8. MR1994532

[66] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen, *Hidden translation and translating coset in quantum computing*, SIAM J. Comput. **43** (2014), no. 1, 1–24, https://doi.org/10.1137/130907203.

[67] D. Garber, D. Kahrobaei, and H. T. Lam, *Length-based attacks in polycyclic groups*, J. Math. Cryptol. **9** (2015), no. 1, 33–43, DOI 10.1515/jmc-2014-0003. MR3318546

[68] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, and U. Vishne, *Length-based conjugacy search in the braid group*, Algebraic methods in cryptography, 2006, pp. 75–87, https://doi.org/10.1090/conm/418/07947.

[69] P. B. Garrett, *Making, breaking codes: Introduction to cryptology*, 1st ed., Prentice Hall PTR, USA, 2000.

[70] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford Ser. (2) **20** (1969), 235–254, DOI 10.1093/qmath/20.1.235. MR248801

[71] M. Garzon and Y. Zalcstein, *The complexity of Grigorchuk groups with application to cryptography*, Theoret. Comput. Sci. **88** (1991), no. 1, 83–98, DOI 10.1016/0304-3975(91)90074-C. MR1130373

[72] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. Algebra **292** (2005), no. 1, 282–302, DOI 10.1016/j.jalgebra.2005.02.002. MR2166805

[73] V. Gebhardt and J. González-Meneses, *Solving the conjugacy problem in Garside groups by cyclic sliding*, J. Symbolic Comput. **45** (2010), no. 6, 629–656, https://doi.org/10.1016/j.jsc.2010.01.013.

[74] S. M. Gersten and H. B. Short, *Rational subgroups of biautomatic groups*, Ann. of Math. (2) **134** (1991), no. 1, 125–158, DOI 10.2307/2944334. MR1114609

[75] É. Ghys and P. de la Harpe (eds.), *Sur les groupes hyperboliques d'après Mikhael Gromov* (French), Papers from the Swiss Seminar on Hyperbolic Groups held in Bern, 1988, Progress in Mathematics, vol. 83, Birkhäuser Boston, Inc., Boston, MA, 1990, DOI 10.1007/978-1-4684-9167-8. MR1086648

[76] R. Gitik, *Nielsen generating sets and quasiconvexity of subgroups*, J. Pure Appl. Algebra **112** (1996), no. 3, 287–292, https://doi.org/10.1016/0022-4049(96)00148-X. MR1410179

[77] S. Gogioso and A. Kissinger, *Fully graphical treatment of the quantum algorithm for the hidden subgroup problem*, arXiv 1701:08669 (2017).

[78] J. González-Meneses, *Improving an algorithm to solve multiple simultaneous conjugacy problems in braid groups*, Geometric methods in group theory, Contemp. Math., vol. 372, Amer. Math. Soc., Providence, RI, 2005, pp. 35–42, DOI 10.1090/conm/372/06872. MR2139675

[79] J. González-Meneses, *Basic results on braid groups*, Ann. Math. Blaise Pascal **18** (2011), no. 1, 15–59, https://doi.org/10.5802/ambp.293.

[80] J. González-Meneses and M. Silvero, *Polynomial braid combing*, Math. Comp. **88** (2019), no. 318, 2027–2045, https://doi.org/10.1090/mcom/3392.

[81] E. Green, *Graph products of groups*, PhD Thesis (1990).

[82] E. Greendlinger and M. Greendlinger, *On Dehn presentations and Dehn algorithms*, Illinois J. Math. **30** (1986), no. 2, 360–363. MR840134

[83] R. I. Grigorčuk, *On Burnside's problem on periodic groups* (Russian), Funktsional. Anal. i Prilozhen. **14** (1980), no. 1, 53–54. MR565099

[84] R. I. Grigorchuk, *On the Milnor problem of group growth* (Russian), Dokl. Akad. Nauk SSSR **271** (1983), no. 1, 30–33. MR712546

[85] R. I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), no. 5, 939–985. MR764305

[86] R. Grigorchuk and D. Grigoriev, *Key agreement based on automaton groups*, Groups Complex. Cryptol. **11** (2019), no. 2, 77–81, DOI 10.1515/gcc-2019-2012. MR4026474

[87] R. I. Grigorchuk and J. S. Wilson, *The conjugacy problem for certain branch groups* (English, with Russian summary), Tr. Mat. Inst. Steklova **231** (2000), no. Din. Sist., Avtom. i Beskon. Gruppy, 215–230; English transl., Proc. Steklov Inst. Math. **4(231)** (2000), 204–219. MR1841756

[88] R. I. Grigorchuk and A. Żuk, *On a torsion-free weakly branch group defined by a three state automaton*, Internat. J. Algebra Comput. **12** (2002), no. 1-2, 223–246, DOI 10.1142/S0218196702001000. International Conference on Geometric and Combinatorial Methods in Group Theory and Semigroup Theory (Lincoln, NE, 2000). MR1902367

[89] D. Grigoriev, *Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines*, Theoret. Comput. Sci. **180** (1997), no. 1-2, 217–228, DOI 10.1016/S0304-3975(96)00188-0. MR1453867

[90] D. Grigoriev and I. Ponomarenko, *Constructions in public-key cryptography over matrix groups*, Algebraic methods in cryptography, Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 103–119, DOI 10.1090/conm/418/07949. MR2389292

[91] D. Grigoriev and V. Shpilrain, *Authentication schemes from actions on graphs, groups, or rings*, Ann. Pure Appl. Logic **162** (2010), no. 3, 194–200, DOI 10.1016/j.apal.2010.09.004. MR2740680

[92] M. Gromov, *Hyperbolic groups*, Essays in group theory, 1987, pp. 75–263, https://doi.org/10.1007/978-1-4613-9586-7_3.

[93] K. W. Gruenberg, *Two theorems on Engel groups*, Proc. Cambridge Philos. Soc. **49** (1953), 377–380, https://doi.org/10.1017/s0305004100028528.

[94] J. Gryak and D. Kahrobaei, *The status of polycyclic group-based cryptography: a survey and open problems*, Groups Complex. Cryptol. **8** (2016), no. 2, 171–186, DOI 10.1515/gcc-2016-0013. MR3567873

[95] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034, DOI 10.2307/2318778. MR327901

[96] M. Habeeb, D. Kahrobaei, C. Koupparis, and V. Shpilrain, *Public key exchange using semidirect product of (semi) groups*, Applied cryptography and network security, 2013, pp. 475–486.

[97] M. Habeeb, D. Kahrobaei, and V. Shpilrain, *A secret sharing scheme based on group presentations and the word problem*, Computational and combinatorial group theory and cryptography, Contemp. Math., vol. 582, Amer. Math. Soc., Providence, RI, 2012, pp. 143–150, DOI 10.1090/conm/582/11557. MR2987392

[98] F. Haglund and D. T. Wise, *Special cube complexes*, Geom. Funct. Anal. **17** (2008), no. 5, 1551–1620, https://doi.org/10.1007/s00039-007-0629-4.

[99] D. Hart, D. Kim, G. Micheli, G. Pascual-Perez, C. Petit, and Y. Quek, *A practical cryptanalysis of WalnutDSA*$^{\text{TM}}$, Public-key cryptography—PKC 2018. Part I, Lecture Notes in Comput. Sci., vol. 10769, Springer, Cham, 2018, pp. 381–406, DOI 10.1007/978-3-319-76578-5_13. MR3781016

[100] K. Hauschild and W. Rautenberg, *Interpretierbarkeit in der Gruppentheorie*, Algebra Universalis **1** (1971/72), 136–151, https://doi.org/10.1007/BF02944970.

[101] G. Havas and M. R. Vaughan-Lee, *4-Engel groups are locally nilpotent*, Internat. J. Algebra Comput. **15** (2005), no. 4, 649–682, DOI 10.1142/S0218196705002475. MR2160572

[102] H. Heineken, *Eine Bemerkung über engelsche Elemente* (German), Arch. Math. (Basel) **11** (1960), 321, DOI 10.1007/BF01236951. MR125153

[103] H. Heineken, *Engelsche Elemente der Länge drei*, Illinois J. Math. **5** (1961), 681–707, http://projecteuclid.org/euclid.ijm/1255631589. MR0131469

[104] S. Hermiller and J. Meier, *Algorithms and geometry for graph products of groups*, J. Algebra **171** (1995), no. 1, 230–257, https://doi.org/10.1006/jabr.1995.1010. MR1314099

[105] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung, *Proactive public key and signature systems*, Proceedings of the 4th ACM conference on Computer and communications security, CCS '97 (1997), 100–110.

[106] M. Hirvensalo, *Quantum computing*, 2nd ed., Natural Computing Series, Springer-Verlag, Berlin, 2004, DOI 10.1007/978-3-662-09636-9. MR2248224

[107] J. Hoffstein, J. Pipher, and J. H. Silverman, *An introduction to mathematical cryptography*, 2nd ed., Undergraduate Texts in Mathematics, Springer, New York, 2014, DOI 10.1007/978-1-4939-1711-2. MR3289167

[108] D. Hofheinz and R. Steinwandt, *Cryptanalysis of a public key cryptosystem based on Grigorchuk group*, Unpublished.

[109] D. Hofheinz and R. Steinwandt, *A practical attack on some braid group-based cryptographic primitives*, Public key cryptography—PKC 2003, Lecture Notes in Comput. Sci., vol. 2567, Springer, Berlin, 2002, pp. 187–198, DOI 10.1007/3-540-36288-6_14. MR2171926

[110] D. F. Holt, B. Eick, and E. A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005, DOI 10.1201/9781420035216. MR2129747

[111] J. M. Howie, *Fundamentals of semigroup theory*, London Mathematical Society Monographs. New Series, vol. 12, The Clarendon Press, Oxford University Press, New York, 1995. Oxford Science Publications. MR1455373

[112] J. Hughes, *The left SSS attack on Ko-Lee-Cheon-Han-Kang-Park key agreement protocol in B45*, Rump Session, Crypto 2000 (2000).

[113] J. Hughes and A. Tannenbaum, *Length-based attacks for certain group based encryption rewriting systems, Workshop SECI02 Sécurité de la communication sur internet*, 2002.

[114] G. Ivanyos, F. Magniez, and M. Santha, *Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem*, 2003, pp. 723–739, https://doi.org/10.1142/S0129054103001996.

[115] D. Kahrobaei and B. Khan, *Nis05-6: A non-commutative generalization of ElGamal key exchange using polycyclic groups*, IEEE Globecom, 2006, pp. 1–5.

[116] D. Kahrobaei and C. Koupparis, *Non-commutative digital signatures*, Groups Complex. Cryptol. **4** (2012), no. 2, 377–384, DOI 10.1515/gcc-2012-0019. MR3043439

[117] D. Kahrobaei and H. T. Lam, *Heisenberg groups as platform for the AAG key-exchange protocol*, 22nd International Conference on Network Protocols (ICNP), IEEE (2014), 660–664.

[118] D. Kahrobaei and K. Mallahi-Karai, *Some applications of arithmetic groups in cryptography*, Groups Complex. Cryptol. **11** (2019), no. 1, 25–33, DOI 10.1515/gcc-2019-2002. MR4000595

[119] D. Kahrobaei and M. Noce, *Algorithmic problems in Engel groups and cryptographic applications*, Int. J. Group Theory **9** (2020), no. 4, 231–250. MR4223607

[120] D. Kahrobaei and V. Shpilrain, *Using semidirect product of (semi)groups in public key cryptography*, Computability in europe 2016: Pursuit of the universal, 2016, pp. 132–141, https://doi.org/10.1007/978-3-319-40189-8_14.

[121] D. Kahrobaei and M. Stanojkovski, *Cryptographic multilinear maps using pro-p groups*, Adv. Math. Commun. **17** (2023), no. 5, 1101–1114, DOI 10.3934/amc.2021041. MR4576170

[122] D. Kahrobaei, A. Tortora, and M. Tota, *Multilinear cryptography using nilpotent groups*, Elementary theory of groups and group rings, and related topics, De Gruyter Proc. Math., De Gruyter, Berlin, [2020] ©2020, pp. 127–133, DOI 10.1515/9783110638387-013. MR4204987

[123] I. Kapovich, *Detecting quasiconvexity: algorithmic aspects*, Geometric and computational perspectives on infinite groups (Minneapolis, MN and New Brunswick, NJ, 1994), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 25, Amer. Math. Soc., Providence, RI, 1996, pp. 91–99, DOI 10.1090/dimacs/025/07. MR1364182

[124] I. Kapovich and N. Benakli, *Boundaries of hyperbolic groups*, Combinatorial and geometric group theory (New York, 2000/Hoboken, NJ, 2001), 2002, pp. 39–93, https://doi.org/10.1090/conm/296/05068.

[125] I. Kapovich, A. Miasnikov, P. Schupp, and V. Shpilrain, *Average-case complexity and decision problems in group theory*, Adv. Math. **190** (2005), no. 2, 343–359, DOI 10.1016/j.aim.2003.02.001. MR2102661

[126] C. Kassel and V. Turaev, *Braid groups*, Graduate Texts in Mathematics, vol. 247, Springer, New York, 2008, https://doi.org/10.1007/978-0-387-68548-9.

[127] A. Keromytis and M. Yung (eds.), *Applied cryptography and network security*, ACNS 2005, Lecture Notes in Comput. Sci., vol. 3531, Springer, Berlin, Heidelberg.

[128] S. Kijima, Y. Otachi, T. Saitoh, and T. Uno, *Subgraph isomorphism in graph classes*, Discrete Math. **312** (2012), no. 21, 3164–3173, DOI 10.1016/j.disc.2012.07.010. MR2957936

[129] S.-h. Kim and T. Koberda, *Embedability between right-angled Artin groups*, Geom. Topol. **17** (2013), no. 1, 493–530, DOI 10.2140/gt.2013.17.493. MR3039768

[130] A. Kitaev, *Quantum computations: algorithms and error correction*, Uspekhi Mat. Nauk **52** (1997), no. 6(318), 53–112, https://doi.org/10.1070/RM1997v052n06ABEH002155.

[131] K. Ko, S. Lee, J. Cheon, J. Han, J. Kang, and C. Park, *New public-key cryptosystem using braid groups*, Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), 2000, pp. 166–183, https://doi.org/10.1007/3-540-44598-6_10.

[132] K. H. Ko, J. W. Lee, and T. Thomas, *Towards generating secure keys for braid cryptography*, Des. Codes Cryptogr. **45** (2007), no. 3, 317–333, DOI 10.1007/s10623-007-9123-0. MR2350533

[133] T. Koberda, *Right-angled groups and their subgroups*, Unpublished notes, https://faculty.virginia.edu/Koberda/raagcourse.pdf.

[134] J. Köbler, U. Schöning, and J. Torán, *The graph isomorphism problem: its structural complexity*, Progress in Theoretical Computer Science, Birkhäuser Boston, Inc., Boston, MA, 1993, DOI 10.1007/978-1-4612-0333-9. MR1232421

[135] N. Koblitz, *Algebraic aspects of cryptography*, with an appendix by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato, Algorithms Comput. Math. **3** (1998), Springer-Verlag, Berlin. MR1610535

[136] M. Kotov, A. Menshov, and A. Ushakov, *An attack on the Walnut digital signature algorithm*, Des. Codes Cryptogr. **87** (2019), no. 10, 2231–2250, https://doi.org/10.1007/s10623-019-00615-y.

[137] M. Kotov and A. Ushakov, *Analysis of a certain polycyclic-group-based cryptosystem*, J. Math. Cryptol. **9** (2015), no. 3, 161–167, DOI 10.1515/jmc-2015-0013. MR3403498

[138] K. Kulesza and Z. Kotulski, *Addressing new challenges by building security protocols around graphs*, Security protocols, Lecture Notes in Comput. Sci., vol. 3364, Springer, Berlin, 2005, pp. 301–306, DOI 10.1007/11542322_36. MR2214280

[139] G. Kuperberg, *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, SIAM J. Comput. **35** (2005), no. 1, 170–188, DOI 10.1137/S0097539703436345. MR2178804

[140] S. J. Lee and E. Lee, *Potential weaknesses of the commutator key agreement protocol based on braid groups*, Advances in cryptology—EUROCRYPT 2002 (Amsterdam), Lecture Notes in Comput. Sci., vol. 2332, Springer, Berlin, 2002, pp. 14–28, DOI 10.1007/3-540-46035-7_2. MR1975525

[141] Y. G. Leonov, *The conjugacy problem in a class of* 2*-groups*, Mat. Zametki **64** (1998), no. 4, 573–583, https://doi.org/10.1007/BF02314631.

[142] P. Lescot, *Isoclinism classes and commutativity degrees of finite groups*, J. Algebra **177** (1995), no. 3, 847–869, https://doi.org/10.1006/jabr.1995.1331.

[143] F. W. Levi, *Groups in which the commutator operation satisfies certain algebraic conditions*, J. Indian Math. Soc. (N.S.) **6** (1942), 87–97. MR7417

[144] L. Levin, *Universal sorting problems*, Problems of Information Transmission **9** (1973), 265–266.

[145] F. Levy-dit Vehel and L. Perret, *On the Wagner-Magyarik cryptosystem*, Coding and cryptography, 2006, pp. 316–329, https://doi.org/10.1007/11779360_25.

[146] H. Liebeck, *Concerning nilpotent wreath products*, Proc. Cambridge Philos. Soc. **58** (1962), 443–451. MR139656

[147] H.-N. Liu, C. Wrathall, and K. Zeger, *Efficient solution of some problems in free partially commutative monoids*, Inform. and Comput. **89** (1990), no. 2, 180–198, DOI 10.1016/0890-5401(90)90010-F. MR1080848

[148] P. Longobardi and M. Maj, *Semigroup identities and Engel groups*, Groups St. Andrews 1997 in Bath, II, London Math. Soc. Lecture Note Ser., vol. 261, Cambridge Univ. Press, Cambridge, 1999, pp. 527–531, DOI 10.1017/CBO9780511666148.016. MR1676649

[149] A. Lubotzky, S. Mozes, and M. S. Raghunathan, *The word and Riemannian metrics on lattices of semisimple groups*, Inst. Hautes Études Sci. Publ. Math. **91** (2000), 5–53 (2001). MR1828742

[150] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Classics in Mathematics, Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition, DOI 10.1007/978-3-642-61896-3. MR1812024

[151] K. Madlener and F. Otto, *Using string-rewriting for solving the word problem for finitely presented groups*, Inform. Process. Lett. **24** (1987), no. 5, 281–284, DOI 10.1016/0020-0190(87)90149-9. MR882625

[152] A. Mal'cev, *On homomorphisms onto finite groups*, Trans. Amer. Math. Soc **119** (1983), 67–79.

[153] T. Mecham and A. Mukherjee, *Hyperbolic groups which fiber in infinitely many ways*, Algebr. Geom. Topol. **9** (2009), no. 4, 2101–2120, DOI 10.2140/agt.2009.9.2101. MR2551664

[154] J. Milnor, *Growth of finitely generated solvable groups*, J. Differential Geometry **2** (1968), 447–449, http://projecteuclid.org/euclid.jdg/1214428659.

[155] J. Milnor, *A note on curvature and fundamental group*, J. Differential Geometry **2** (1968), 1–7, http://projecteuclid.org/euclid.jdg/1214501132.

[156] M. R. R. Moghaddam, A. R. Salemkar, and K. Chiti, *n-isoclinism classes and n-nilpotency degree of finite groups*, Algebra Colloq. **12** (2005), no. 2, 255–261, DOI 10.1142/S1005386705000246. MR2127250

[157] G Moussong, *Hyperbolic Coxeter groups*, ProQuest LLC, Ann Arbor, MI, 1988. Thesis (Ph.D.)–The Ohio State University, http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:8824577.

[158] A. Myasnikov, V. Shpilrain, and A. Ushakov, *A practical attack on a braid group based cryptographic protocol*, Advances in cryptology—CRYPTO 2005, Lecture Notes in Comput. Sci., vol. 3621, Springer, Berlin, 2005, pp. 86–96, DOI 10.1007/11535218_6. MR2237301

[159] A. Myasnikov and A. Weiß, TC^0 *circuits for algorithmic problems in nilpotent groups*, 42nd International Symposium on Mathematical Foundations of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 83, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2017, pp. Art. No. 23, 14. MR3755316

[160] A. Myasnikov, V. Shpilrain, and A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*, with an appendix by Natalia Mosina, Mathematical Surveys and Monographs, vol. 177, American Mathematical Society, Providence, RI, 2011, DOI 10.1090/surv/177. MR2850384

[161] A. Myasnikov and V. Roman'kov, *A linear decomposition attack*, Groups Complex. Cryptol. **7** (2015), no. 1, 81–94, https://doi.org/10.1515/gcc-2015-0007.

[162] A. Myasnikov, V. Shpilrain, and A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*, with an appendix by Natalia Mosina, Mathematical Surveys and Monographs, vol. 177, American Mathematical Society, Providence, RI, 2011, DOI 10.1090/surv/177. MR2850384

[163] A. Myasnikov and A. Ushakov, *Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld key exchange protocol*, Public key cryptography—PKC 2007, Lecture Notes in Comput. Sci., vol. 4450, Springer, Berlin, 2007, pp. 76–88, DOI 10.1007/978-3-540-71677-8_6. MR2404113

[164] A. Myasnikov and A. Ushakov, *Random subgroups and analysis of the length-based and quotient attacks*, J. Math. Cryptol. **2** (2008), no. 1, 29–61, DOI 10.1515/JMC.2008.003. MR2451658

[165] A. Miasnikov and S. Vassileva, *Log-space conjugacy problem in the Grigorchuk group*, Groups Complex. Cryptol. **9** (2017), no. 1, 77–85, DOI 10.1515/gcc-2017-0005. MR3641682

[166] L. Narendra-Mohan and G. S. G. N. Anjaneyulu, *A secured digital signature using conjugacy and DLP on non-commutative group over finite field*, Advances in Intelligent Systems and Computing (AISC) **516** (2017), 449–465.

[167] B. B. Newman, *Some results on one-relator groups*, Bull. Amer. Math. Soc. **74** (1968), 568–571, DOI 10.1090/S0002-9904-1968-12012-9. MR222152

[168] W. Nickel, *Computation of nilpotent Engel groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 2, 214–222. Group theory. MR1717415

[169] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000. MR1796805

[170] NIST, *Post-Quantum Cryptography PQC*, 2020. https:\csrc.nist.gov/projects/post-quantum-cryptography.

[171] P. S. Novikov and S. I. Adjan, *Infinite periodic groups. I–III*, Mathematics of the USSR-Izvestiya **2** (1968).

[172] E. O'Brien, *Polycyclic groups.* https://www.icts.res.in/sites/default/files/1284624569notes.pdf.

[173] R. O'Donnell, *Quantum computation and quantum information*, 2018, https://www.cs.cmu.edu/~odonnell/quantum18/.

[174] R. Ostrovsky and W. E. Skeith III, *Communication complexity in algebraic two-party protocols*, Advances in cryptology—CRYPTO 2008, Lecture Notes in Comput. Sci., vol. 5157, Springer, Berlin, 2008, pp. 379–396, DOI 10.1007/978-3-540-85174-5_21. MR2490385

[175] D. Panagopoulos, *A secret sharing scheme using groups*, arXiv 1009.0026v1 (2010).

[176] A. L. T. Paterson, *Amenability*, Mathematical Surveys and Monographs, vol. 29, American Mathematical Society, Providence, RI, 1988, DOI 10.1090/surv/029. MR961261

[177] C. Petit and J. J. Quisquater, *Cryptographic hash functions and expander graphs: the end of the story?*, The new codebreakers, 2016, pp. 304–311, https://doi.org/10.1007/978-3-662-49301-4_19.

[178] G. Petrides, *Cryptanalysis of the public key cryptosystem based on the word problem on the Grigorchuk groups*, Cryptography and coding, Lecture Notes in Comput. Sci., vol. 2898, Springer, Berlin, 2003, pp. 234–244, DOI 10.1007/978-3-540-40974-8_19. MR2090936

[179] S. J. Pride, *Small cancellation conditions satisfied by one-relator groups*, Math. Z. **184** (1983), no. 2, 283–286, DOI 10.1007/BF01252863. MR716277

[180] N. Rahman and V. Shpilrain, *MAKE: a matrix action key exchange*, J. Math. Cryptol. **16** (2022), no. 1, 64–72, DOI 10.1515/jmc-2020-0053. MR4360035

[181] O. Regev, *Quantum computation and lattice problems*, SIAM J. Comput. **33** (2004), no. 3, 738–760, https://doi.org/10.1137/S0097539703440678.

[182] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, J. ACM **56** (2009), no. 6, Art. 34, 40, https://doi.org/10.1145/1568318.1568324.

[183] V. N. Remeslennikov, *Conjugacy in polycyclic groups* (Russian), Algebra i Logika **8** (1969), 712–725. MR280593

[184] E. Rips, *Subgroups of small cancellation groups*, Bull. London Math. Soc. **14** (1982), no. 1, 45–47, DOI 10.1112/blms/14.1.45. MR642423

[185] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), no. 2, 120–126, https://doi.org/10.1145/359340.359342.

[186] D. J. S. Robinson, *A course in the theory of groups*, Second, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996, https://doi.org/10.1007/978-1-4419-8594-1.

[187] M. Roetteler and T. Beth, *Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups*, arXiv quant-ph:9812070 (1998).

[188] V. Roman'kov, *A linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups*, arXiv 1501:01152 (2015).

[189] A. V. Rozhkov, *The conjugacy problem in an automorphism group of an infinite tree*, Mat. Zametki **64** (1998), no. 4, 592–597, https://doi.org/10.1007/BF02314633.

[190] P. E. Schupp, *A survey of small cancellation theory*, Word problems: decision problems and the Burnside problem in group theory (Conf., Univ. California, Irvine, Calif., 1969; dedicated to Hanna Neumann), Stud. Logic Found. Math., Vol. 71, North-Holland, Amsterdam-London, 1973, pp. 569–589. MR412289

[191] D. Segal, *Decidable properties of polycyclic groups*, Proc. London Math. Soc. (3) **61** (1990), no. 3, 497–528, DOI 10.1112/plms/s3-61.3.497. MR1069513

[192] Z. Sela, *The isomorphism problem for hyperbolic groups. I*, Ann. of Math. (2) **141** (1995), no. 2, 217–283, https://doi.org/10.2307/2118520.

[193] H. Servatius, *Automorphisms of graph groups*, J. Algebra **126** (1989), no. 1, 34–60, https://doi.org/10.1016/0021-8693(89)90319-0.

[194] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 124–134, DOI 10.1109/SFCS.1994.365700. MR1489242

[195] V. Shpilrain and A. Ushakov, *The conjugacy search problem in public key cryptography: unnecessary and insufficient*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 3-4, 285–289, DOI 10.1007/s00200-006-0009-6. MR2233787

[196] V. Shpilrain and A. Ushakov, *A new key exchange protocol based on the decomposition problem*, Algebraic methods in cryptography, Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 161–167, DOI 10.1090/conm/418/07954. MR2389297

[197] V. Shpilrain and G. Zapata, *Combinatorial group theory and public key cryptography*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 3-4, 291–302, DOI 10.1007/s00200-006-0006-9. MR2233788

[198] H. Sibert, P. Dehornoy, and M. Girault, *Entity authentication schemes using braid word reduction*, Discrete Appl. Math. **154** (2006), no. 2, 420–436, DOI 10.1016/j.dam.2005.03.015. MR2194414

[199] C. Staecker, *Dehn.gap, http://cstaecker.fairfield.edu/ cstaecker/files/gap/dehn.gap*.

[200] D. R. Stinson, *Cryptography*, 3rd ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. Theory and practice. MR2182472

[201] R. Strebel, *Appendix. Small cancellation groups*, Sur les groupes hyperboliques d'après Mikhael Gromov (Bern, 1988), Progr. Math., vol. 83, Birkhäuser Boston, Boston, MA, 1990, pp. 227–273. MR1086661

[202] D. A. Suprunenko and M. S. Garaščuk, *Linear groups with Engel's condition* (Russian), Dokl. Akad. Nauk BSSR **6** (1962), 277–280. MR143818

[203] S. Sze, D. Kahrobaei, R. Dambreville, and M. Dupas, *Finding n-th roots in nilpotent groups and applications in cryptology*, Int. J. Pure Appl. Math. **70** (2011), no. 4, 571–593. MR2848462

[204] T. tom Dieck, *Transformation groups*, De Gruyter Studies in Mathematics, vol. 8, Walter de Gruyter & Co., Berlin, 1987, DOI 10.1515/9783110858372.312. MR889050

[205] B. Tsaban, *Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography*, J. Cryptology **28** (2015), no. 3, 601–622, DOI 10.1007/s00145-013-9170-9. MR3355794

[206] L. Van Wyk, *Graph groups are biautomatic*, J. Pure Appl. Algebra **94** (1994), no. 3, 341–352, https://doi.org/10.1016/0022-4049(94)90015-9.

[207] N. R. Wagner and M. R. Magyarik, *A public-key cryptosystem based on the word problem*, Advances in cryptology (Santa Barbara, Calif., 1984), 1985, pp. 19–36, https://doi.org/10.1007/3-540-39568-7_3.

[208] J. S. Wilson, *Two-generator conditions for residually finite groups*, Bull. London Math. Soc. **23** (1991), no. 3, 239–248, https://doi.org/10.1112/blms/23.3.239.

[209] J. S. Wilson and P. A. Zalesskii, *Conjugacy separability of certain torsion groups*, Arch. Math. (Basel) **68** (1997), no. 6, 441–449, https://doi.org/10.1007/s000130050076.

[210] J. A. Wolf, *Growth of finitely generated solvable groups and curvature of Riemannian manifolds*, J. Differential Geometry **2** (1968), 421–446, http://projecteuclid.org/euclid.jdg/1214428658.

[211] C. Wrathall, *The word problem for free partially commutative groups*, J. Symbolic Comput. **6** (1988), no. 1, 99–104, DOI 10.1016/S0747-7171(88)80024-5. MR961373

[212] P. Zhu and Q. Wen, *Affine braid groups: a better platform than braid groups for cryptology?*, Appl. Algebra Engrg. Comm. Comput. **22** (2011), no. 5-6, 375–391, DOI 10.1007/s00200-011-0157-1. MR2863392

[213] M. Zorn, *Nilpotency of finite groups*, Bull. Amer. Math. Soc. **42** (1936), 485–486.

Index

$Cat(k)$-space, 78
δ-neighborhood, 75
δ-slim, 76

Action
  Effective, 8
  Free, 8
  Transitive, 8
Algorithmic problems in graphs and groups, 16
  Arboricity, 18
  Clique problem, 17
  Decomposition problem, 17
  Geodesic length problem, 16
  Graph coloring, 17
  Independent set problem, 17
  Induced subgroup isomorphism problem, 17
  Snake-in-the-box problem, 17
  Subdivision problem, 17
  Subgroup distortion problem, 16
  Vertex cover problem, 18
Anshel-Anshel-Goldfeld protocol, 33, 72
Arboricity, 107
Artin generators, 77
Artin presentation, 66
Automorphism, 4

Brute force attack, 47

CAKE, 90
Cardinality, 5
Cayley graph, 76
Center, 7
Centralizer, 7
Chromatic number, 107
Classical cryptography, 21
  Diffie-Hellman key exchange, 23
  Digital signature scheme, 25
    ElGamal, 26
    RSA, 25
  ElGamal encryption, 24
  Multilinear maps, 28
    Applications, 29
    Nilpotent groups, 30
  RSA cryptosystem, 22
  Secret sharing schemes, 27
    Shamir's secret sharing scheme, 28
Commensurable, 109
Commutator, 10
Commutator key exchange problem, 49, 52
Comparison point, 78
Comparison triangle, 78
Computational basis, 53
Computational problems
  Graph automorphism problem, 57
  Hidden shift problem, 61
  Hidden subgroup problem, 53
  Semidirect discrete logarithm problem, 60
  Semigroup discrete logarithm problem, 58
  Vectorization problem, 61
Conjugacy problem, 40, 71
Coset, 6
Cryptanalysis, 47
Cubical complex, 103
Cyclically reduced word, 85

Decision problems, 13, 51
  n-th root problem, 15
  Bounded geodesic length problem, 105
  Conjugacy problem, 15
  Dehn's decision problems, 15
  Endomorphism decision problem, 15
  Epimorphism problem, 15
  Generalized word problem, 15
  Geodesic length problem, 82
  Geodesic problem, 82
  Group homomorphism problem, 15
  Isomorphism problem, 15
  Membership problem, 82
  Power decision problem, 15
  Rational subset memebership problem, 15
  Subgroup intersection problem, 16
  Subgroup membership decision problem, 15

Vertex cover problem, 107
Word problem, 15, 33
Decomposition problem, 34
Decryption function, 21, 22
Degree of n-nilpotency, 18
Dehn algorithm, 79
Dehn filling, 79
Dehn presentation, 79
Diffie-Hellman problem, 23
Digital signatures, 38
Direct product, 4
Discrete log problem, 18, 23, 24, 27

Eilenberg-MacLane space, 103
Encryption function, 21, 22
Endomorphism, 4
Engel element, 115

Field, 4
Fixed point, 8
Free group, 13

Garside normal form, 68
Generalized discrete log problem, 18
Generator, 4
Geodesic length, 16, 48
Geodesic triangle, 75
Graph metric, 76
Greedlinger's lemma, 87
Group, 3
n-Engel, 116
p, 37
Abelian, 3
Arithmetic, 109
Artin-Tits, 65, 77
Basilica, 125
Baumslag-Solitar, 78
Biautomatic, 103
Braid, 33, 65
Burnside, 117
Coxeter, 77
Cyclic, 4
Dihedral, 56
Engel, 115
Exponentially distorted, 84
Finitely generated, 6
Fuchsian, 77
General linear group, 5
Graph, 101
Graph braid, 104
Grigorchuk, 126
Heisenberg, 10, 33, 56
Hyperbolic, 75
Infinite, 57
Isotropy, 8
Left-orderable, 67
Linear algebraic, 109
Nilpotent, 10, 115
Periodic, 6
Permutation, 56
Polycyclic, 35, 93
Quotient, 6
Self-similar, 121
Small cancellation, 86
Solvable, 56
Special linear group, 5
Surface, 77
Symmetric, 4
Torsion, 6
Torsion free, 6
Undistorted, 105
Group action, 8
Group presentation, 14
1-Relator groups, 14
Examples, 14
Finitely presented groups, 14
Preperfect, 103

Hadamard gate, 55
Hash function, 39
Hidden shift problem, 58
Hirsch length, 94
Holomorph, 36
Homomorphism, 4
Hyperbolic manifold, 78

Image, 9
Index, 6

Kernel, 9
Known-plaintext attack, 112
Ko, Lee, et al. key exchange, 34, 72

Learning homomorphism problem with noise, 18
Learning with errors problem, 18
Length function, 76
Length of a word, 16
Length-based attack, 34, 47
Best descend (LBA), 48
Generalized LBA, 48
LBA with backtracking, 48
Linear centralizer attack, 49
Linear decomposition attack, 37, 50
Applications, 51
Logspace, 105

Metric condition, 86
Metric space, 75
Monoid, 3
Multilinear Diffie-Hellman assumption, 30
Multilinear map, 118
Multitape Turing machine, 80

Nielsen transformation, 44
Noncommutative ElGamal, 35
Normal form, 102
Normal subgroup, 7
Normalizer, 7

One-way function, 22
Orbit, 8
Order, 5

Partial measurement, 54
Piece, 86
Piling
  Pyramidal, 104
  Viennot, 104
Polly Cracker scheme, 107
Polycyclic presentation, 95
Polycyclic series, 94
Public-key cryptography, 22

Quantum Fourier transform, 56
Quantum register, 54
Quasi-monotone conjugacy property, 80
Quasiconvex, 82
Qubit, 53
Quotient attack, 51

Rips construction, 82

Search problems, 13, 16
  Conjugacy search problem, 16, 34, 35, 72
  Membership search problem, 52
  Power conjugacy search problem, 16, 36
  Simultaneous conjugacy search problem, 16, 34, 52
  Subgroup-restricted simultaneous conjugacy search problem, 49, 72
  Word search problem, 16
Secret sharing, 42
Semidirect product, 36, 60
Semigroup, 3, 59
Shor's algorithm, 54
Short exact sequence, 9
Shortlex ordering, 43
Small cancellation condition, 86
Special generators, 102
Stabilizer, 8
Staecker implementation, 89
Strand, 66
Stretching factor, 81
Subgroup, 5
Symmetrized closure, 86
Symmetrized subset, 85

Tensor product, 54
Thue system, 103
Thurston norm, 83
Tietze transformations, 90
Tree, 121
Triangle condition, 86

Ultra summit set, 71
Unipotent, 110
Unique shortest vector problem, 58

Virtually unipotent, 110

Word problem, 44

278 **Delaram Kahrobaei, Ramón Flores, Marialaura Noce, Maggie E. Habeeb, and Christopher Battarbee,** Applications of Group Theory in Cryptography, 2024

277 **George Metcalfe, Francesco Paoli, and Constantine Tsinakis,** Residuated Structures in Algebra and Logic, 2023

276 **Balázs Bárány, Károly Simon, and Boris Solomyak,** Self-similar and Self-affine Sets and Measures, 2023

275 **Alekos Vidras and Alain Yger,** Multidimensional Residue Theory and Applications, 2023

274 **Willi Freeden and M. Zuhair Nashed,** Recovery Methodologies: Regularization and Sampling, 2023

273 **Gennadiy Feldman,** Characterization of Probability Distributions on Locally Compact Abelian Groups, 2023

272 **Tadashi Ochiai,** Iwasawa Theory and Its Perspective, Volume 1, 2023

271 **Hideto Asashiba,** Categories and Representation Theory, 2022

270 **Leslie Hogben, Jephian C.-H. Lin, and Bryan L. Shader,** Inverse Problems and Zero Forcing for Graphs, 2022

269 **Ralph S. Freese, Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor,** Algebras, Lattices, Varieties, 2022

268 **Ralph S. Freese, Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor,** Algebras, Lattices, Varieties, 2022

267 **Dragana S. Cvetković Ilić,** Completion Problems on Operator Matrices, 2022

266 **Kate Juschenko,** Amenability of Discrete Groups by Examples, 2022

265 **Nabil H. Mustafa,** Sampling in Combinatorial and Geometric Set Systems, 2022

264 **J. Scott Carter and Seiichi Kamada,** Diagrammatic Algebra, 2021

263 **Vugar E. Ismailov,** Ridge Functions and Applications in Neural Networks, 2021

262 **Ragnar-Olaf Buchweitz,** Maximal Cohen–Macaulay Modules and Tate Cohomology, 2021

261 **Shiri Artstein-Avidan, Apostolos Giannopoulos, and Vitali D. Milman,** Asymptotic Geometric Analysis, Part II, 2021

260 **Lindsay N. Childs, Cornelius Greither, Kevin P. Keating, Alan Koch, Timothy Kohl, Paul J. Truman, and Robert G. Underwood,** Hopf Algebras and Galois Module Theory, 2021

259 **William Heinzer, Christel Rotthaus, and Sylvia Wiegand,** Integral Domains Inside Noetherian Power Series Rings, 2021

258 **Pramod N. Achar,** Perverse Sheaves and Applications to Representation Theory, 2021

257 **Juha Kinnunen, Juha Lehrbäck, and Antti Vähäkangas,** Maximal Function Methods for Sobolev Spaces, 2021

256 **Michio Jimbo, Tetsuji Miwa, and Fedor Smirnov,** Local Operators in Integrable Models I, 2021

255 **Alexandre Boritchev and Sergei Kuksin,** One-Dimensional Turbulence and the Stochastic Burgers Equation, 2021

254 **Karim Belabas and Henri Cohen,** Numerical Algorithms for Number Theory, 2021

253 **Robert R. Bruner and John Rognes,** The Adams Spectral Sequence for Topological Modular Forms, 2021

252 **Julie Déserti,** The Cremona Group and Its Subgroups, 2021

251 **David Hoff,** Linear and Quasilinear Parabolic Systems, 2020

250 **Bachir Bekka and Pierre de la Harpe,** Unitary Representations of Groups, Duals, and Characters, 2020

This book is intended as a comprehensive treatment of group-based cryptography accessible to both mathematicians and computer scientists, with emphasis on the most recent developments in the area. To make it accessible to a broad range of readers, the authors started with a treatment of elementary topics in group theory, combinatorics, and complexity theory, as well as providing an overview of classical public-key cryptography. Then some algorithmic problems arising in group theory are presented, and cryptosystems based on these problems and their respective cryptanalyses are described. The book also provides an introduction to ideas in quantum cryptanalysis, especially with respect to the goal of post-quantum group-based cryptography as a candidate for quantum-resistant cryptography.

The final part of the book provides a description of various classes of groups and their suitability as platforms for group-based cryptography.

The book is a monograph addressed to graduate students and researchers in both mathematics and computer science.

ISBN 978-1-4704-7469-0
9 781470 474690
SURV/278

For additional information
and updates on this book, visit
www.ams.org/bookpages/surv-278